

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

REMARKS

Claims 1, 3-8 and 10-41 are pending in the patent application, of which claims 15-41 were withdrawn from consideration. As such, Claims 1, 3-8 and 10-14 are under consideration.

Claims 3, 4, 10 and 11 were objected due to certain informalities. The claims have been amended as suggested by the Examiner to overcome the objections.

Claims 1, 3-8 and 10-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over USPN 5,809,139 to Girod et al. (hereinafter “Girod”) in view of USPN 5,742,685 to Berson et al. (hereinafter “Berson”). Rejection of the claims is respectfully traversed because the references, alone or in combination, do not disclose or suggest all of the limitations of the claims.

As per Claim 1, Girod does not teach all of the claimed limitations. Further, Applicant respectfully maintains that Berson is non-analogous art and not reasonably pertinent to the present invention because Berson is directed to an identification card and a system for producing and authenticating such an identification card. According to Berson, a person whom the identification card will identify, is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The signal representing the image is encrypted using a public key encryption system and the key is downloaded from a

center. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. (Abstract). Despite the Patent Office's interpretation, Berson is not in the field of the invention. For example, as discussed below, Berson does not even relate to protecting a transmitted signal from illicit use.

Further, by contrast, the present invention provides a system for copy protecting a digital signal representing audiovisual information. For example, Berson does not teach the limitations of "transmitting the scrambled signal and said data signal to a receiver," as required by Claim 1. The audiovisual digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal, and the scrambled signal and said CP data signal are transmitted to a receiver.

However, in Berson an encryption key E_i and an encoded decryption key $X[D_i]$ are transferred from center 40 to encrypter module 20. In contrast, according to the claimed invention, a signal that is scrambled and copy protected, and the CP data signal, are transmitted to the receiver.

It is respectfully submitted that the Patent Office's interpretation of Berson is improper. Nowhere in Berson are the limitations of "transmitting the scrambled signal and said data signal

to a receiver" according to Claim 1, taught or suggested. In col. 3 line 57 to col. 4, line 25,

Berson states that:

"Text input 30 provides text message T and at least a portion of text message T, which preferably includes other personal information such as name, address, license number, etc. relating to person P, is combined with the compressed form of the first signal to form the second signal which is encrypted by encrypter module 20 to provide encrypted information $E_i[M]$ [L]ike image I text T is embodied in card C in both humanly recognizable form on the front CF and coded and encrypted form on the back CB of card C. In a preferred embodiment of the subject invention a data center 40 transmits encryption code E_i to encrypter module 20.... To facilitate decryption of encrypted information $E_i[M]$ data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information $E_i[M]$ by coder module 22... [W]hen card C is to be verified the necessary decryption key D_i can be obtained by decrypting encrypted decryption key $X[D_i]$" (emphasis added).

According to Berson, the image I and text T are embodied in card C in both humanly recognizable form on the front CF and coded and encrypted form on the back CB of card C. In the preferred embodiment of FIG. 1, the data center 40 transmits encryption code E_i to the encrypter module 20. For later decryption of encrypted information $E_i[M]$, the data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information $E_i[M]$ by coder module 22. When later the card C is to be verified, the necessary decryption key D_i can be obtained by decrypting encrypted decryption key $X[D_i]$. Therefore, the data center 40 sends encryption key E_i and decryption key D_i to the encrypter module 20, such that the encrypted information $E_i[M]$ and decryption key D_i are placed on the card for later validation of the card.

In response to Applicant's prior arguments the Patent Office relies on Berson (col. 4, lines 9-12) to interpret Berson as "sending $E_i[M]$ and $X[D_i]$ ", wherein $E_i[M]$ is the encrypted data and $E_i[M]$ and $X[D_i]$ is the decryption key. However, in col. 4, lines 9-12 Berson only states that: "To facilitate decryption of encrypted information $E_i[M]$ data center 40 also transmits an encrypted decryption key $X[D_i]$ to be appended to the encrypted information $E_i[M]$ by coder module 22." It is respectfully submitted that as discussed above and shown in FIG. 1, Berson (col. 3, line 57 to col. 4, line 25) clearly states that the data center 40 transmits: (1) the encryption key E_i to the encrypter 20 and (2) the encrypted decryption key $X[D_i]$ to the coder module 22 to be appended to the encrypted information $E_i[M]$. The encrypted information $E_i[M]$ is not sent by the data center 40 to the apparatus 10. Rather, the encrypted information $E_i[M]$ is generated by the encrypter 20 within the apparatus 10. The data center 40 does not generate or contain the encrypted information $E_i[M]$, let alone sending it to the apparatus 10.

According to Berson, a person whom the identification card will identify, is scanned to produce a digital signal which is compressed, encrypted, and coded as a two dimensional barcode or as some other appropriate form of coding, which is incorporated into one portion of the identification card. The signal representing the image is encrypted using a public key encryption system and the key is downloaded from the center. To validate the card the coded message is scanned, decoded, decrypted, expanded and displayed. (Abstract).

Consistent with Applicants reading of Berson, in FIG. 1 Berson designates the line from the data center 10 that leads to the encrypter 20 in the apparatus 10 as carrying the encryption key E_i . Further, that same line from the data center 10 to the coder 22 is designated to also carry the encrypted decryption key $X[D_i]$. There is no line from data center 40 to the apparatus 10 that is designated as carrying the encrypted information $E_i[M]$.

This difference is further shown by FIG. 2 of Berson which shows apparatus 50 for validating the identification card C. The back CB of card C is scanned by a barcode scanner 52 having the capability to scan an appropriate two dimensional barcode. The scanned signal is then decoded by decoder module 54 and decrypted by decrypter module 58. Key X (or keys) is obtained by decrypter 58 from center 40. According to Col. 4, lines 9-12 of Berson (relied upon by the Patent Office), the data center 40 does not send out copy protected, encrypted information, AND a data signal to be used to remove the copy protection. The data center only provides encryption and decryption keys to encrypter 20. This is totally different than the present invention.

By contrast, the present invention provides a system for copy protecting a digital signal representing audiovisual information, including the limitations of “transmitting the scrambled signal and said data signal to a receiver,” as required by Claim 1. The audiovisual digital signal is first encoded to obtain an encoded signal, and the encoded signal is converted into a copy protected signal using a copy protection function (the copy protection function utilizes a CP data

signal representing copy protection data). Then the copy protected signal is scrambled to obtain a scrambled signal, and the scrambled signal and said CP data signal are transmitted to a receiver. There is no such teaching in Berson.

The Office Action recognizes the advantages of the presently claimed invention by trying to make modifications in Girod and Berson “to facilitate removal of the watermark in Girod by including the frequency spreading signal with the transmitted data”. It is well settled that in order for a modification or combination of the prior art to be valid, the prior art itself must suggest the modification or combination, “...invention cannot be found obvious unless there was some explicit teaching or suggestion in the art to motivate one of ordinary skill to combine elements so as to create the same invention.” *Winner International Royalty Corp. v. Wang*, No. 96-2107, 48 USPQ.2d 1139, 1140 (D.C.D.C. 1998) (emphasis added). “The prior art must provide one of ordinary skill in the art the motivation to make the proposed molecular modifications needed to arrive at the claimed compound.” *In re Jones*, 958 F.2d 347, 21 USPQ.2d 1941, 1944 (Fed. Cir. 1992) (emphasis added). Neither of the references suggests the motivation to modify or combine the references as proposed. Girod and Berson are individually complete and functionally independent for their limited specific purposes and there would be no reason to make the modification proposed by the Office Action. Therefore, because neither of the prior art references suggests the combination and modifications proposed by the Office Action the combination and modifications are improper.

There is no motivation in Girod of including the frequency spreading signal with the transmitted data. Further, the Patent Office does not explain how “including the frequency spreading signal with the transmitted data” can be accomplished Girod according to Berson. Berson only provides a method and apparatus for producing and authenticating an identification card. As detailed above, the signal representing a person’s image is encrypted using a public key encryption system and placed on an ID card. For decryption, the key is downloaded from a center. As such, not only

Even if the modification was legally justified, it still would not render Applicants’ claimed invention obvious. The Office Action admits that Girod does not teach all limitations in Claim 1. Therefore, the Office Action attempts to modify Girod in order to teach Applicants’ claimed invention. However, as discussed, there is no teaching in Girod and or Berson of the claimed limitations. Berson teaches away from the present invention. Accordingly, the effort required to combine the teachings of Girod and Berson would require a substantial undertaking and numerous elements which would not be obvious.

Further, Applicant respectfully submits that the Office Action is improperly using “hindsight” and the teachings of Applicant’s own claimed invention in order to combine references to render Applicants’ claims obvious. The Office Action admits that Girod fails to teach all of the limitations of Applicant’s claimed invention. However, the Office Action improperly attempts to modify Girod using Berson (which also fails to teach all of the limitations

of Applicant's claimed invention), in an attempt to achieve Applicant's claimed invention.

Finally, if Applicants' claimed invention were in fact obvious, those skilled in the art would have modified the teachings of Girod to incorporate the teachings of Berson. The fact that neither reference has been modified, to implement Applicants' claimed invention, despite its great advantages, indicates that Applicant's claimed invention is neither obvious nor taught by the prior art. Therefore, for at least the above reasons, Claim 1 is patentably distinct from the cited references, alone or in combination. Accordingly, rejection of Claim 1, and dependent claims therefrom, should be withdrawn.

As per Claim 3, for example, the limitation of "transmitting the scrambled signal and said data signal as a single signal" is not disclosed or suggested by the references, alone or combination, for reasons provided in relation to Claim 1. **As per Claim 4**, the limitation of "combining the scrambled signal and said data signal into said single signal" is not disclosed by the references, alone or combination, for reasons provided in relation to Claim 1. If Claims 3 and 4 are again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of each claim.

As per Claim 6, according to Claim 1 on which Claim 6 is dependent, initially a digital signal is copy protected by: (a) encoding the digital signal to obtain an encoded signal; (b)

converting the encoded signal into a copy protected signal using a copy protection function, wherein the function utilizes a data signal representing copy protection data; (c) scrambling the copy protected signal to obtain a scrambled signal; and (d) transmitting the scrambled signal and said data signal to a receiver. The present invention offers the flexibility of using copy protection data to introduce copy protection, and then use the transmitted copy protection data, to recover/remove the copy protection, according to Claim 6.

Girod does not disclose “descrambling the scrambled signal to recover said copy protected signal”, as required by Claim 6. Girod does not disclose “reconverting the recovered copy protected signal back into the encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal”, as required by Claim 6. Girod does not disclose “decoding the converted encoded signal to recover said digital signal,” as required by Claim 6.

By contrast, in relation to Figure 1 (relied upon by the Patent Office), Girod states:

“The input to the system is either a digital video signal or an analog video signal...” (col. 3, lines 49-52);

“The digital video signal (either original or converted using A/D converter 8) is then input to a video coder 10, which is one of a number of different known digital video compression coders” (col. 3, lines 55-58); and

“Referring again to FIG. 1, the output of the interframe coder 10 is input to either digital watermarking apparatus 26 or data storage device 24” (col. 4, lines 60-62).

Then in conjunction with Figures 1 and 2c, in col. 5, lines 7-10 of Girod (relied upon by the Patent Office), Girod states:

“Once the signal is watermarked, it is transmitted to the receiver in question. The received signal can then be decoded at the destination site using interframe video decoder 28. The decoder 28 performs the inverse functions of the coder 10, in a manner well understood in the art. The watermark, having been embedded in the digital signal, can be recovered later in a manner described below.”

Clearly, in Figures 1 and 2c and col. 5, lines 7-10, Girod does not disclose “descrambling the scrambled signal to recover said copy protected signal”, as required by Claim 6. Further, Girod does not disclose “reconverting the recovered copy protected signal back into the encoded signal using an inverse copy protection function, wherein the inverse function utilizes copy protection data from said copy protection data signal”, as required by Claim 6. Recovering copy protection data allows use of that data by a reconverter to reconvert the copy protected signal. Indeed, Girod does not disclose an inverse copy protection function that utilizes copy protection data from the copy protection data signal provided by a transmitter. And, Girod does not disclose “decoding the converted encoded signal to recover said digital signal,” as required by Claim 6. The Patent Office is reading steps of the claimed invention into Girod, and as is clear from above, those steps do not exist in Girod. Therefore, for at least these reasons, Claim 6 should be allowed.

As per Claims 5, 7, 12 and 14, at least the limitations in parts (a)-(d) of Claim 5, parts (a)-(e) of Claim 7, parts (a)-(d) of Claim 12, and parts (a)-(c) of Claim 14, are not taught or suggested by the references, alone or combination, for the above reasons. The Patent Office has not shown where these limitations are disclosed in the references. For at least these reasons and the reasons provided above, rejections of Claims 5, 7, 12 and 14 should be withdrawn. If Claims 5, 7, 12 and 14 are again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of each claim.

As per Claim 8, for the same reasons provided above in relation to Claim 1, rejection of Claim 8, and dependent claims therefrom, should be withdrawn.

As per Claim 10, the claimed limitations of a combiner for combining the scrambled signal and said data signal into said single signal, and a transmitter for transmitting said single signal, are not disclosed or suggested by the references, alone or combination, for reasons provided in relation to Claim 1. If Claims 10 is again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of the claim.

As per Claim 11, the limitation of a transmitter for transmitting the scrambled signal and

said data signal as a single signal, is not disclosed or suggested by the referenced, alone or in combination, for reasons provided in relation to Claim 1. If Claim 11 is again rejected, Applicant respectfully requests that the Patent Office refer to such specific limitations in the references, if they exist, and provide specific reasons for rejection of the claim.

As per Claim 13, the above arguments in relation to rejection Claim 6, are incorporated herein, in response to rejection of Claim 13. Therefore, for at least these reasons, Claim 13 should be allowed.

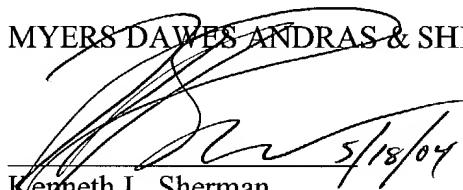
Conclusion

Please charge any additional fees or credit any overpayment to our Deposit Account No. 01-1960. A duplicate copy of this page is enclosed for that purpose.

Re-examination, reconsideration and allowance of all claims are respectfully requested.

Respectfully submitted,

MYERS DAWES ANDRAS & SHERMAN, LLP


5/18/04
Kenneth L. Sherman
Registration No. 33,783
19900 MacArthur Blvd.
Eleventh Floor
Irvine, CA 92612
Telephone: (949) 223-9600
Facsimile: (949) 223-9610

R:\M-Z\SAM1\SAM1.PAU.58\05AMD.5-4-04.doc

I hereby certify that this correspondence is being deposited with the United States Postal Services first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231, on May 18, 2004
P.O. Box 450, Alexandria, VA 22313 Date
By Susan M. Dangworth
May 18, 2004
Date of Signature